Quantum Cloning, Eavesdropping and Bell's inequality

N. Gisin and B. Huttner
Group of Applied Physics
University of Geneva
20 Rue de l'Ecole de Medecine
CH 1211 Geneva 4
Switzerland

20/11/1996

Abstract

We analyze various eavesdropping strategies on a quantum cryptographic channel. We present the optimal strategy for an eavesdropper restricted to a two-dimensional probe, interacting on-line with each transmitted signal. The link between safety of the transmission and the violation of Bell's inequality is discussed. We also use a quantum copying machine for eavesdropping and for broadcasting quantum information.

1 Introduction

How good can a quantum "photocopy machine" be? How many pairs of people can use such a machine on a given 2-particle source and still violate Bell's inequality? How much information can an eavedroper read out of a quantum cryptography channel for a given BER (bit error rate)? Is quantum privacy amplification intrinsically more powerful than its classical analog, or is it only provably secure? How much are the above questions related to each other?

This letter plays with the above questions and provides several answers that in turn raise more questions. The general motivation stems from quantum cryptography, but the problematic is more general: what can one do with quantum information that can not be done with classical information? Indeed, quantum information processing calls for original applications, not just mimicking classical applications in a more efficient way. Shor's factorization algorithm [1], for example, is certainly not the end of the adventure, but a brilliant step that calls for more (realistic) imagination.

The paradigm of this letter is a source of entangled EPR particles, assumed to be spin half particles, now known as qubits, which are shared between two users, known as Alice and Bob. One particle goes directly to Alice, while the other one may be modified on its way to Bob by a malevolent eavesdropper, known as Eve. Alice and Bob may now use various setups, either to distribute a secret key, or to test "the inequality" [1] [2]. The choice of setups on both sides is summarized in Fig. 1. In the so-called BB84 or 4-states protocol for quantum cryptography [3], Alice measures her particles, either in the vertical basis: $\updownarrow$, or in the horizontal one: $\leftrightarrow$. She chooses her basis at her free will (or using a "true" random generator), independently of all other players in the protocol. Equivalently, we could assume that Alice prepares particles in either basis and send them to Bob. This would be entirely equivalent for our purposes. Bob does precisely the same as Alice (but making independent choices), thus measuring the particles in either $\updownarrow$ or $\leftrightarrow$ bases. Alternatively, Alice and Bob may choose to use their particles to test the inequality. In this case, Bob simply rotates his reference frame by 45 degrees. Finally, they may use the Ekert protocol for quantum cryptography [4], and choose a combination of both setups, each of them now choosing between three possible bases. In this case, when they both use the same basis, as in the BB84 protocol, they shall use the data to obtain a key, while when they use different bases, they use the data to test the inequality.

[1] When John Bell was talking of his inequality, he would just say "the inequality". We shall adopt the same prescription in this work

To these ideal protocols, we shall add Eve, the malevolent eavesdropper who would like to hear what Alice has to say to Bob. Her aim is to obtain as much information as possible on the key exchanged between Alice and Bob, while creating as little disturbance as possible. Actually Eve has the most interesting position in this game, as, in principle, she is allowed to do everything, being only limited by the laws of physics (and the size of the Universe [5]). However, in order to keep the problem manageable, we shall impose two conditions:

1. She interacts with only one qubit at a time.

2. Her probe can be described by a two-dimensional Hilbert space (i.e. it is also a qubit).

These two restrictions do limit the validity of our approach, but they are also the only realistic ones experimentally. Indeed, it is becoming possible to make two qubits interact with one another [6], but more complicated systems are still quite a way off. A more general case, with an auxiliary system described by a four-dimensional Hilbert space, was recently described by Bužek and Hillery [7], who devised a universal quantum-copying machine (UQCM). We shall compare this machine with a simpler two-dimensional one, and show that the UQCM is only marginally better. Moreover, Fuchs and Peres [8] have recently shown that, as long as the initial state of Eve's probe is a pure state, there is no need to go beyond a four-dimensional space. They have also shown, although only numerically, that the optimal detection method for a two-states system is obtained with a two-dimensional probe only.

In Section 2 we find the optimal strategy for Eve using a two-dimensional probe. This strategy is better than the standard "intercept-resend" strategy. It is also better than a strategy that has recently been published [9], and was refered to as "optimal". The reason is that [9] is restricted to on-line measurements: Eve has to perform her measurement immediately. Here, as we introduce an explicit probe, we also allow Eve to delay her measurement on her probe till Alice and Bob announce publicly the bases they used. We find also that, using this strategy, Eve can get reliable enough data to violate the inequality while Bob's data are still good enough to also violate the inequality! Finally, the result of this Section prove that quantum privacy amplification [10] is fundamentally more efficient than classical error correction and privacy amplification in the sense that for high enough BER, the latter is no longer possible, whereas the former is still efficient. In Section 3 a pretty good quantum-copying machine (PGQCM) machine is presented. The machine itself is classical: only the original qubit and the clone are quantum, each represented by a 2-D Hilbert space. This pretty good machine is then compared to Bužek and Hillery [7] UQCM. The latter requires a quantum machine, albeit the machine can also be described by a 2-D Hilbert space. We lend these two machines to Eve and see that using either one provides her with more information than the standard intercept-resend strategy, but less than the strategy studied in Section 2. Amusingly, we note that using such copy machine Eve can send the (perturbed) original qubit to Bob_1 and the (poor) copy to some Bob_2, both Bobs violating Bell's inequalities (with respect to Alice data) or both Bobs establishing secret crypto keys with Alice. This provides a new way to broadcast quantum information, as depicted in Fig. 2.

2 Eavedropping with a 2-D probe

In this Section we analyze and optimize the following eavedroping strategy for Eve. The general setting is depicted in Fig. 3. When Alice sends a qubit $|\psi\rangle$ to Bob, Eve lets a second qubit (often called the probe or the ancilla) interact with $|\psi\rangle$. Initially Eve's probe is in a know state $|0\rangle$ and the joint state of the unknown qubit and the probe is a product state $|\psi\rangle \otimes |0\rangle$. This product state undergoes some unitary evolution after which the unknown qubit is forwarded to Bob who does his standard measurement, irrespective of Eve's strategy. Eve may either measure her probe immediately, as in the following measurement of intensity γ, or keep her probe until Alice and Bob reveal the bases used to encode this bit, and then measure the probe and gains information about the corresponding bit of the cryptographic key. Of course Eve does not need to use always the same unitary evolution. In this way she can for instance restore the symmetry that some evolution may break. She can also decide to reduce the perturbation, at the cost of reducing in the same ratio her information gain, by probing only a fraction of the unknown qubits (this amounts to choosing the identity as unitary evolution). We shall only consider input states of the form $|\psi(\theta)\rangle = \cos(\theta/2)|\uparrow\rangle + sin(\theta/2)|\downarrow\rangle$. On the Poincaré (or Bloch) sphere these states are represented by

the points of a large circle that passes through the antipodic points representing $|\uparrow\rangle$ and $|\downarrow\rangle$, and θ is the angle between the directions defined by the points representing $|\uparrow\rangle$ and $|\psi\rangle$ (Fig. 4). In this way only real numbers need to be used. The unitary evolution is thus defined by the following real parameters a_j and b_j:

$$\begin{aligned} |\uparrow\rangle \otimes |0\rangle \quad &\rightarrow a_1|\uparrow\uparrow\rangle + a_2|\uparrow\downarrow\rangle + a_3|\downarrow\uparrow\rangle + a_4|\downarrow\downarrow\rangle \\ |\downarrow\rangle \otimes |0\rangle \quad &\rightarrow b_1|\uparrow\uparrow\rangle + b_2|\uparrow\downarrow\rangle + b_3|\downarrow\uparrow\rangle + b_4|\downarrow\downarrow\rangle \end{aligned} \tag{1}$$

where unitarity implies $\sum_j |a_j|^2 = \sum_j |b_j|^2 = 1$ and $\sum_j a_j^* b_j = 0$.

Assuming an $\uparrow\downarrow$ symmetry, one has $b_j = a_{5-j}$. Accordingly the general unitary transformation is determined by only 2 parameters that can be chosen as follows:

$$\begin{aligned} a_1 &= \cos\alpha\cos\beta \qquad a_2 = \cos\alpha\sin\beta \\ a_3 &= \sin\alpha\cos\beta \qquad a_4 = -\sin\alpha\sin\beta \end{aligned} \tag{2}$$

For example the standard Von Neumann measurements correspond to $\alpha = \beta = 0$. This example can be generalized to another interesting case: $\alpha = 0$ and $\cos(\beta)^2 = \frac{1+\sin\gamma}{2}$; γ ranges between 0 and $\pi/2$. We call this *measurements of intensity* γ, as γ parametrizes the amount of information that Eve may obtain from her probe. We shall see below that, if we restrict Eve to a 2-D probe, this kind of measurement optimizes Eve's information gain at low BERs, and is practically indistinguishable from the optimum up to a BER of about 15%. First, let us rewrite the measurement of intensity γ as follows, see Fig. 4:

$$\begin{aligned} |\uparrow\rangle \otimes |0\rangle \quad &\rightarrow |\uparrow\rangle \otimes |\psi(\frac{\pi}{2} - \gamma)\rangle \\ |\downarrow\rangle \otimes |0\rangle \quad &\rightarrow |\downarrow\rangle \otimes |\psi(\frac{\pi}{2} + \gamma)\rangle \end{aligned} \tag{3}$$

When Alice sends state $|\psi(\theta)\rangle$, which corresponds to the following density matrix:

$$\rho_{\text{Alice}} = \frac{1}{2}\begin{pmatrix} 1+\cos\theta & \sin\theta \\ \sin\theta & 1-\cos\theta \end{pmatrix}, \tag{4}$$

the states at the disposal of Bob and Eve, obtained by tracing out the other's qubit, read:

$$\rho_{\text{Bob}} = \frac{1}{2}\begin{pmatrix} 1+\cos\theta & \cos\gamma\sin\theta \\ \cos\gamma\sin\theta & 1-\cos\theta \end{pmatrix} \tag{5}$$

$$\rho_{\text{Eve}} = \frac{1}{2}\begin{pmatrix} 1+\sin\gamma\cos\theta & \cos\gamma \\ \cos\gamma & 1-\sin\gamma\cos\theta \end{pmatrix} \tag{6}$$

For $\gamma = 0$ Eve does not introduce any errors in the transmission (the density matrix of Bob is unchanged), but does not gain any information either (her density matrix becomes independent of the initial state). For positive γ some information about θ can be gained by measuring Eve's probe and for γ approaching $\pi/2$ this information is the optimum Von Neumann scheme (from the information point of view). Simultaneously, Eve's interception introduces a perturbation on the initial state $\psi(\theta)$, as shown by Eqs. (4) and (5). We see that when Alice and Bob use the $\updownarrow$ basis ($\theta = 0$ or $\theta = \pi$), Eve introduces no perturbation: the state received by Bob is unchanged. However, she gains information. For example, the a posteriori probability of having input state $|\uparrow\rangle$, once she has found her probe in the $|\uparrow\rangle$ state is:

$$P(\psi = \uparrow | \text{probe} = \uparrow) = \frac{1+\sin(\gamma)}{2}. \tag{7}$$

On the other hand, when Alice and Bob choose the $\leftrightarrow$ basis ($\theta = \pm\pi/2$), Eve introduces errors, but gains no information at all (same ρ_{Eve} for both inputs). Hence Eve gains nothing by waiting until she knows the bases: she can measure her probe immediately after it interacted with the unknown qubit. This is a very significant practical advantage of the measurements of intensity γ. Assuming that Alice and Bob chose either bases with frequency 50%, Eve's overall information gain is:

$$I_{AE}(\gamma) = \frac{1}{2}\left[1 + \frac{1+\sin\gamma}{2}\log_2(\frac{1+\sin\gamma}{2}) + \frac{1-\sin\gamma}{2}\log_2(\frac{1-\sin\gamma}{2})\right], \tag{8}$$

where $\log_2$ is the base two logarithm, to get the information in bits.

A problem associated with these measurements however, is that the error rate depends on the basis used by Alice and Bob. Therefore, by checking it independently for the two bases, Alice and Bob may infer that the noise in their transmission is not produced by a random process. Moreover they may get some information about Eve's strategy. To avoid that, Eve should use a random combination of two measurement strategies, one along the $\updownarrow$ axis, as in Eq. (4), and one along the $\leftrightarrow$ axis. It is easy to see that, for this second strategy, the density matrix of the state received by Bob becomes:

$$\rho'_{\rm Bob} = \frac{1}{2}\begin{pmatrix} 1+\cos\gamma\cos\theta & \sin\theta \\ \sin\theta & 1-\cos\gamma\cos\theta \end{pmatrix} , \tag{9}$$

so that the final density matrix, for the random combination of both strategies is:

$$\overline{\rho}_{\rm Bob} = \frac{1}{2}\begin{pmatrix} 1+\eta\cos\theta & \eta\sin\theta \\ \eta\sin\theta & 1-\eta\cos\theta \end{pmatrix} , \tag{10}$$

where $\eta \equiv \frac{1+\cos\gamma}{2}$. This density matrix is now entirely symmetric with respect to the initial state. Indeed, if we write the initial density matrix: $\rho_{\rm Alice} = \frac{1+\vec{m}\cdot\vec{\sigma}}{2}$, where $\vec{m} = (\sin\theta, 0, \cos\theta)$ is the Bloch vector representating $\rho_{\rm Alice}$ on the Poincaré sphere, the final state is: $\overline{\rho}_{\rm Bob} = \frac{1+\eta\vec{m}\cdot\vec{\sigma}}{2}$. The effect of Eve's eavesdropping is thus simply to "shrink" the Bloch vector by η.

The disturbance of the initial state increases with increasing γ, as indicated by the fidelity function:

$$\mathcal{F}(\gamma) \equiv \langle\psi(\theta)|\overline{\rho}_{\rm Bob}|\psi(\theta)\rangle = \frac{3+\cos\gamma}{4} , \tag{11}$$

or equivalently by the BER, $q(\gamma)$:

$$q(\gamma) \equiv 1 - \mathcal{F}(\gamma) = \frac{1-\cos(\gamma)}{4} . \tag{12}$$

Eve's information gain, Eq. (8), as a function of the BER, Eq. (12), is depicted on Fig. 5, together with Bob's information: $I_{AB} = 1 + q\log_2 q + (1-q)\log_2(1-q)$. Fig. 5 shows that, above a BER of about 15%, Eve may have more info than Bob, hence no classical error correction and privacy amplification can be applied. It is interesting to note that this simple strategy is undistinguishable from the "optimal" strategy of [9].

In order to discover the quality of the simple measurements of intensity γ, we performed a computer optimization of Eve's information I_{AE} for given BERs, assuming the most general eavesdropping strategy given by Eqs. (2) and (3). In this case, the density matrix received by Bob when Alice sends state $|\psi(\theta)\rangle$ is:

$$\rho_{\rm Bob} = \frac{1}{2}\begin{pmatrix} 1+\cos\theta\cos 2\alpha & \sin 2\alpha\cos 2\beta + \sin\theta\cos 2\alpha\sin 2\beta \\ \sin 2\alpha\cos 2\beta + \sin\theta\cos 2\alpha\sin 2\beta & 1-\cos\theta\cos 2\alpha \end{pmatrix} . \tag{13}$$

The density matrix received by Eve is simply obtained by interchanging $\alpha \longleftrightarrow \beta$. Similarly to the measurement of intensity γ, in order to avoid creating an assymmetric state for Bob, Eve has to use a random combination of strategies. In this case, she has to choose at random between four possible unitary transformations similar to Eq. (2), corresponding to four choices of symmetry breaking along four directions mutually orthogonal on the Poincaré sphere (e.g. $\uparrow$, $\downarrow$, $\leftarrow$, $\rightarrow$). The averaged density matrix for Bob becomes similar to Eq. (10), with $\eta = \frac{\cos 2\alpha(1+\sin 2\beta)}{2}$. Note that, for this more general strategies, Eve gains information in both bases, $\updownarrow$ and $\leftrightarrow$. However, since this information is different for the two bases, it is now preferable for Eve to wait till Alice and Bob announce their bases publicly, before she measures her probe. The calculation of I_{AE} as a function of α and β is more cumbersome but straightforward, and will not be presented here explicitely. The computer optimization, giving the best I_{AE} at a given error rate, is represented by the upper curve of Fig. 5. The optimum strategy for Eve is a measurement of intensity γ for low error rates, and remains indistinguishable from it up to a BER of about 15%. For example, at the crossing point between I_{AB} and I_{AE}, i.e. for a BER of 0.1534, $I^{\gamma}_{AE} = 0.3816$, while $I^{\rm opt}_{AE} = 0.3820$. However, above this BER value, Eve can get more information. In particular for large BER she can get more than 0.5 bits of information.

Let us now look at the case where Alice and Bob wish to test the inequality to check the integrity of the transmission. Following the above discussion, and since we are mainly interested in low error rates, we shall restrict ourselves to the measurement of intensity γ. Let us first analyze the inequality mentionned in the introduction (see Fig. 1), where the reference frames of Alice and Bob are rotated by 45°. Eve's symmetry axis, i.e. her choice of $\uparrow$ and $\downarrow$ states in Eq. 2, may be chosen along any of the axes chosen by Alice and Bob. We can easily calculate the value of the parameter S that appears in the CHSH version of Bell's inequality [11], to get:

$$S_{AB} = \sqrt{2}(1 + \cos\gamma) \, , \tag{14}$$

(The same value is also obtained when Eve adopts the symmetrized strategy). This shows that if the BER is less than $q_{\rm Bell} = 1/2 - \sqrt{2}/4 \approx 0.1464$, Alice and Bob's data violates the inequality. On the other hand, for the particular setup of Fig. 1(b), for a BER above $q_{\rm Bell}$, their data does not violate the inequality.

The above discussion only refers to the particular setup of Fig. 1(b), where the reference frames of Alice and Bob are at 45°. A more general criterion was recently given by the Horodeckis [12], giving the necessary and sufficient condition for a density matrix to violate the CHSH inequality [11] for at least one particular choice of directions. Applying first this criterion to our *unsymmetrized* system (i.e. Eve uses only one measurement of intensity γ), we found that Alice and Bob's joint density matrix fulfills this criterion for $\gamma < \pi/2$. Therefore, there exists one set of directions following which Alice and Bob would still violate some CHSH inequality till an error rate of 25%. However,if we now consider *symmetrized* strategies, which are more likely to be used by Eve in order to avoid detection, we find that the limit is precisely $q_{\rm Bell}$. In other words, above this limit, the joint density matrix does not violate any CHSH inequality, and the above choice at 45° is optimal for testing for eavesdropping with CHSH inequalities.

The value of $q_{\rm Bell} \approx 0.1464$ is suspiciously close to the intersection of the two curves I_{AB} and I_{AE}, at a BER of 0.1534. Therefore, we make the conjecture that the real optimal strategy, which should be obtained with a 4-D probe, would give this very point[2]. The violation of the inequality would then become a interesting measure of the eavesdropping[3]: if the inequality is violated, Alice and Bob know that Eve has less mutual information than themselves, and that they can in principle perform classical information processing to obtain a secret key. If the inequality is not violated, then Eve may have more information, and so a secret key cannot be distilled by classical means. Note that the conjecture is restricted to symmetrized strategies, so that Alice and Bob still need to check that the error rate is the same for all four possible states. This conjecture is not proven yet, but at least there is no known strategy which contradicts it.

However, even though above an error rate of 0.1464 Alice and Bob cannot extract a secret key by classical information processing, there is still something quantum hidden there. Indeed, using the so-called purification of entanglement [14], Alice and Bob may still take advantage of their system to extract a secret key. This procedure, known as quantum privacy amplification or QPA [10], performs operations on two pairs of particles at a time, and can extract from the corrupted set pairs of entangled states with an arbitrarily high degree of entanglement, on which Eve is automatically excluded. In our case, the condition for this algorithm to be effective reads:

$$\langle\psi_-|\rho|\psi_-\rangle > \frac{1}{2} \, , \tag{15}$$

where $|\psi_-\rangle \equiv \frac{\sqrt{2}}{2}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$ is the singlet state, and ρ the joint density matrix of Alice and Bob. This limit is attained for $\gamma = \pi/2$, corresponding to an error rate of 25%. This proves that QPA is not only "provably secure", but is trully more powerful than any classical privacy amplification algorithm.

Note that if Eve and Bob both do measurements in the diagonal bases, then both Eve and Bob can violate Bell inequality for some values of γ. Indeed when Alice and Bob use the setup of Fig. 1(b), and Eve uses measurements of intensity γ, we find $S_{AE} = 2\sqrt{2}\sin\gamma$. Both S_{AB} and S_{AE} are therefore larger than 2 for γ around $\pi/3$.

[2]This conjecture seems to be validated by very recent results by Fuchs and Peres [13], who analyzed the optimal strategy (obtained with a 4-D probe). Their results show that $I_{AB} = I_{AE}$ for a BER of 0.1464.

[3]This idea was first expressed by A. Ekert

3 Quantum cloning and broadcasting of quantum information

In this Section we consider the question of (imperfect) quantum cloning and its possible application for eavedropping and quantum information broadcasting. First, we consider "classical" quantum cloning machines in which the only relevant quantum degrees of freedom are two qubits, one to be copied and one to receive the copy. Hence, we can use the same general frame as in the previous Section 2, that is the unitary transformation defined by Eq. (2) with the parameters α and β as defined by Eq. (3). In this case, what we want is the two density matrices $\rho_{\rm Bob}$ and $\rho_{\rm Eve}$ to be equal, and as close as possible to the original $\rho_{\rm Alice}$. For the moment, the distinction between Bob and Eve is not relevant, as both now have the same kind of copy of the original state. However, since we later want to use this copying machine for eavesdropping, we keep the terminology. From Eq. (13), the two matrices are equal when $\alpha = \beta$. In order to give a quantitative measure of the quality of our cloning machine, we use the mean fidelity with respect to the perturbed original qubit[4]:

$$\bar{\mathcal{F}} = \frac{1}{2\pi}\int_0^{2\pi} \langle\psi(\theta)|\rho_{\rm Bob}|\psi(\theta)\rangle d\theta \ . \tag{16}$$

It is now straightforward to find the maximum value:

$$\bar{\mathcal{F}}_{\rm opt} = \frac{8+3\sqrt{3}}{16} \approx 0.825 \ , \tag{17}$$

which is reached for $\alpha = \beta = \pi/12$. Interestingly, it is also possible to relax the equality condition, and simply optimize the sum of the fidelities of the two copies. The result is the same as Eq. (17). We like to call this cloning machine a Pretty Good Quantum Copying Machine (PGQCM), for reasons described below.

Fig. 6 displays the Bloch vector corresponding to the copied states for original states corresponding to a large circle on the Poincaré sphere. Note that these are highly non symmetric. However, the symmetry can be restored if the cloning machine uses at random four similar unitary transformation, corresponding to four choices of symmetry breaking along four directions mutually orthogonal (on the Poincaré sphere),similarly to the previous eavesdropping strategy. This amounts to add an additional degree of freedom, but this one can be classical, hence easy to produce in the lab. The Bloch vector with such a copy machine is the same as given in Eq. (17), and is also shown in Fig. 6. In this case the Bloch vectors of the copies are the same, $\vec{m}_{\rm copy}$, and are simply related to the Bloch vector of the original qubit $\vec{m}_{\rm ini}$ by $\vec{m}_{\rm copy} = \eta\vec{m}_{\rm ini}$, where $\eta = 2\bar{\mathcal{F}}_{\rm opt} - 1$.

Recently Bužek and Hillery [7] have introduced another cloning machine, the UQCM (Universal Quantum Cloning Machine). This is a truly quantum mechanical machine in the sense that in addition to the minimum two qubits, the machine itself has quantum degrees of freedom, although these can be described by a 2-D Hilbert space with basis vectors $M_\uparrow$ and $M_\downarrow$. Their machine is described by the following unitary transformation:

$$\begin{aligned} |\uparrow\rangle\otimes|0\rangle\otimes|M\rangle_o &\rightarrow \sqrt{\frac{2}{3}}|\uparrow\uparrow\rangle\otimes|M_\uparrow\rangle + \sqrt{\frac{1}{6}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)\otimes|M_\downarrow\rangle \\ |\uparrow\rangle\otimes|0\rangle\otimes|M\rangle_o &\rightarrow \sqrt{\frac{2}{3}}|\downarrow\downarrow\rangle\otimes|M_\downarrow\rangle + \sqrt{\frac{1}{6}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)\otimes|M_\uparrow\rangle \end{aligned} \tag{18}$$

As for the PGQCM, the density matrices of both copies are equal. Moreover, this machine is already symmetric, with fidelity $\bar{\mathcal{F}}_{\rm uni}$ independent of the initial state:

$$\bar{\mathcal{F}}_{\rm uni} = \frac{5}{6} \approx 0.833 \ . \tag{19}$$

The corresponding Bloch vector is also plotted in Fig. 6. Note that the UQCM has a slightly higher mean fidelity than the PGQCM (about 1% larger) at the cost of the complication due to the additional quantum degree of freedom, hence our vocabulary of "pretty good" for our PGQCM.

[4]This criterion is certainly not the only one that can be adopted, but it gives simple and reasonable results

Eve may use either of these copying machines to tape into Alice and Bob quantum communication channel. Here, contrary to the case of measurement of intensity γ studied in Section 2, Eve gains to wait until Alice and Bob reveal their bases, before measuring her copy. Moreover, for the case of the UQCM, since the state of the machine itself after the interaction depends on the initial state, Eve may use this extra information contained in the machine. Her information gain for given BERs is added on Fig. 5, both for the PGQCM and the UQCM. We see that even the UQCM provide less information than the optimal strategy using only a 2-D probe.

Finally, one may also use either cloning machines to send copies to two different Bobs, let say Bob_1 and Bob_2. Each Bob can then independently measure his qubits. We find out that, when we use the assymetric PGQCM, both Bobs violate the inequality with respect to the same Alice data. It is clear from Fig. 6 that this is dependent on the choice of directions a, a', b and b'. For the symmetrized version, $S_{AB_1} = S_{AB_2} = 2\sqrt{2}(2\bar{\mathcal{F}} - 1) < 2$, so that there is no violation. It should also be noted that the results of Bob_1 and Bob_2 are not independent, because the cloning entangles the original and the clone qubits.

4 Conclusion

The best possible eavesdropping strategy remains to be explored. However, we have seen that even using only one qubit as a probe, i.e. using techniques already under development in several labs, Eve can do better than the standard intercept/resend strategy. We have found the optimal strategy for such probes, and shown that for low BER, it is indistinguishable from a simple strategy termed measurement of intensity γ. This strategy puts a limit of about 15% on the BER above which Eve may possess more information than Bob, which means that classical information processing can not be used to distill a secret key. However, for the same eavesdropping strategy, quantum information processing, and more precisely the QPA may still be used, up to a BER of 25%-ϵ, for any $\epsilon > 0$. Hence, quantum privacy amplification not only enables to distribute the key in a provably secure fashion, but is also intrinsically more powerful than its classical analog. Amusingly, using the strategy described in Section 2, Eve can extract enough information from the quantum channel to violate the inequality, while simultaneously perturbing the quantum channel so little that Bob could still violate the inequality (with respect to the same data of Alice).

Perfect quantum cloning is impossible. However, an arbitrary qubit can be cloned in such a way that both the perturbed original qubit and the cloned qubit both have a fidelity above 80%, independently of the initial state to be copied. Such cloning machine can be used to broadcast quantum information, for quantum cryptography purposes or for the fun of multi-violation of Bell's inequalities. The Pretty Good Quantum Cloning machine presented in Section 3, while about 1% less efficient than the Universal Quantum Copy Machine, is close to feasible with todays technology. Both this PGQCM and the measurement of intensity γ are interesting examples of potential uses for the simplest quantum gates, with only two interacting qubits, which are now under development in various laboratories.

Acknowledgments

We would like to thank A. Peres for a very fruitful discussion, and S. Popescu and T. Mor for useful comments. We gratefully acknowledge financial support from the Swiss Fonds National de Recherche Scientifique.

References

[1] P.Shor, in *Proceedings of the 35th Annual Symposium on the Foundation of Computer Sciences* (IEEE Computer Society, Los Alamitos, CA 1994), p. 124.

[2] J.S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, (Cambridge University Press, 1987).

[3] C.H. Bennett, F. Bessette, G. Brassard, and L. Salvail, J. of Cryptology **5**, 3 (1992)

[4] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[5] I.C. Percival, in*Quantum Chaos, Quantum measurement*, (NATO ASI Series 357, 1992) P.Cvitanovic Ed.

[6] Q.A Turchette, C.J. Hood, W. Lange, H. Mabuchi and H.J.Kimble, Phys. Rev. Lett. **75**, 4710 (1995); C. Monroe, D.M.Meekhof, B.E. King, W.M. Itano and D.J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995).

[7] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).

[8] C.A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).

[9] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996).

[10] D. Deutsch, A. Ekert, R. Jozsa, C. Machiavello, S. Popescu and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[11] J.F. Clauser, M.A. Horne, A. Shimony and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[12] M. Horodecki, P. Horodecki and M. Horodecki, Phys. Lett. A **200**,340 (1995).

[13] C. A. Fuchs and A. Peres, to be published.

[14] C.H. Bennett, H.J. Bernstein, S. Popescu and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

Figures

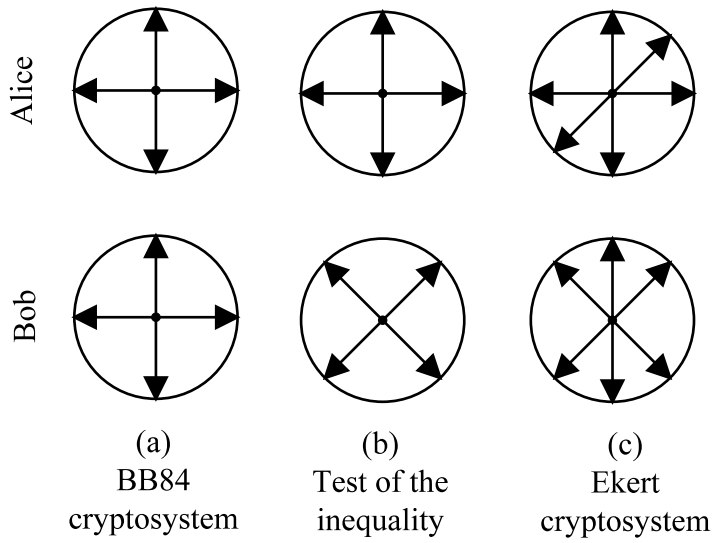

Figure 1: The various setups
To implement the BB84 quantum cryptographic protocol, Alice and Bob use the same bases to prepare and measure their particles. A representation of their states on the Poincaré sphere is shown in (a). A similar setup, but with Bob's bases rotated by 45°, can be used to test the violation of Bell inequality, as shown in (b). Finally, in the Ekert protocol, Alice and Bob may use the violation of Bell inequality to test for eavesdropping, as shown in (c).

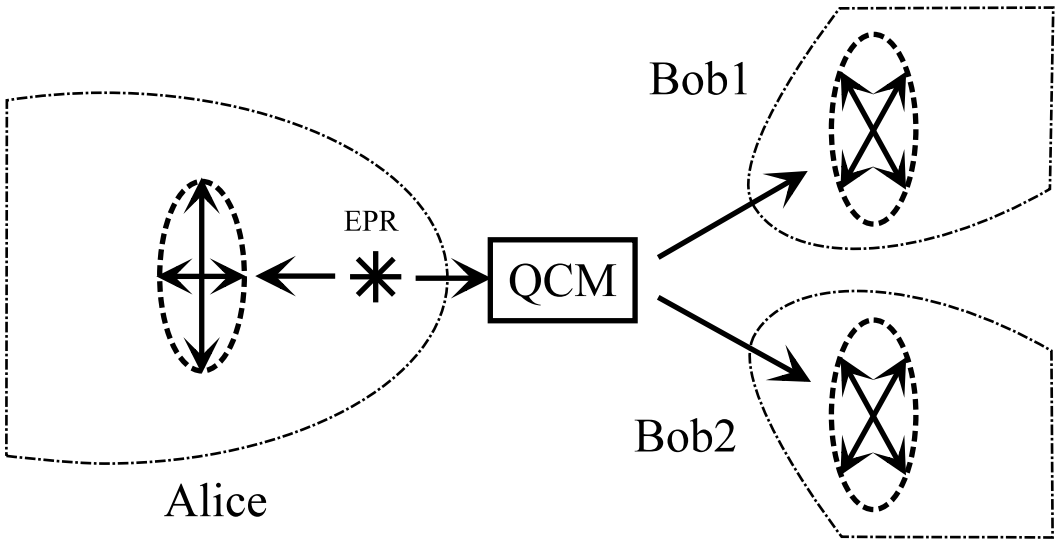

Figure 2: Broadcasting quantum information
Quantum cloning machines (QCM) allow to broadcast quantum information, i.e. share it between various users, at the cost of reducing the fidelity of the channels.

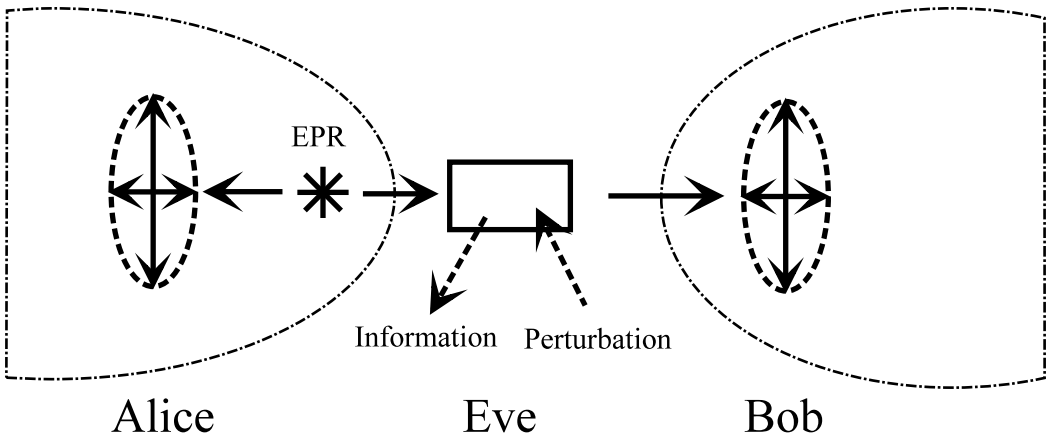

Figure 3: Eavesdropping on a quantum channel
Eve extracts information out of the quantum channel between Alice and Bob at the cost of introducing noise into that channel.

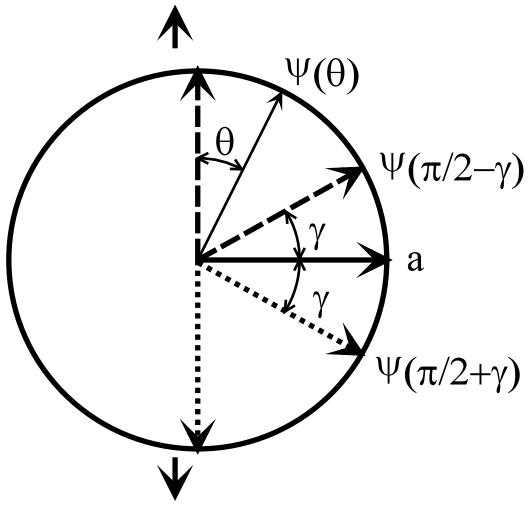

Figure 4:
State of the ancilla after the interaction corresponding to measurements of intensity γ of an $\uparrow$ state (dashed line,$\psi(\pi/2-\gamma)$) and of a $\downarrow$ state (dotted line,$\psi(\pi/2+\gamma)$). **a** corresponds to the symmetry breaking direction of the measurement.

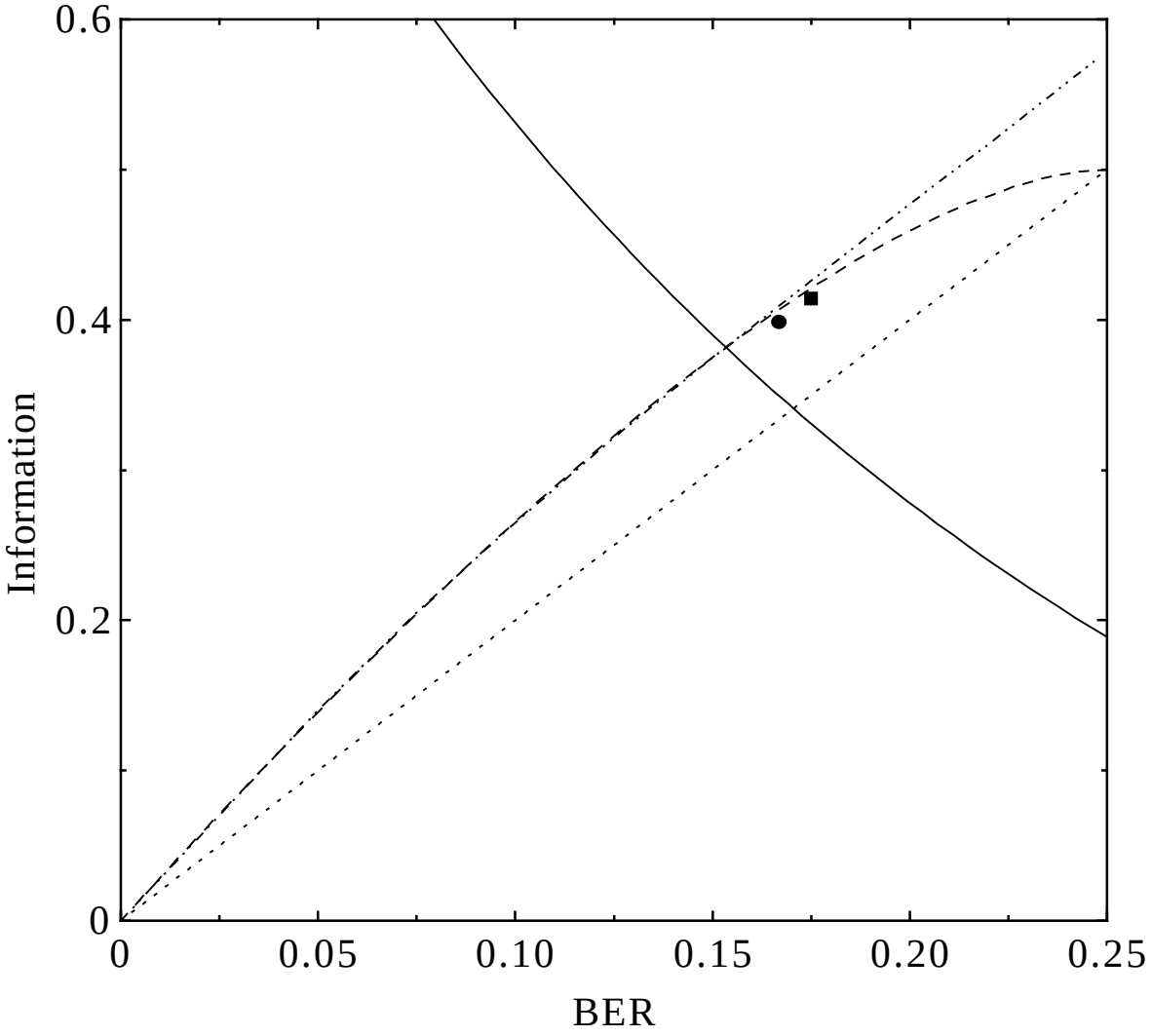

Figure 5:
Information gain versus Bite Error Rate (BER) for various eavesdroping strategies. The full curve represents the mutual information between Alice and Bob. The dotted curve is the information available to Eve for the intercept/resend strategy. The dashed curve is for the measurement of intensity γ. The dashed-dotted curve is the optimal eavesdropping strategy with a 2D probe. The circle is the information gained by Eve if she uses a UQCM (which requires interaction between three qubits), while the square is obtained by the PGQCM (which only requires interaction between two qubits).

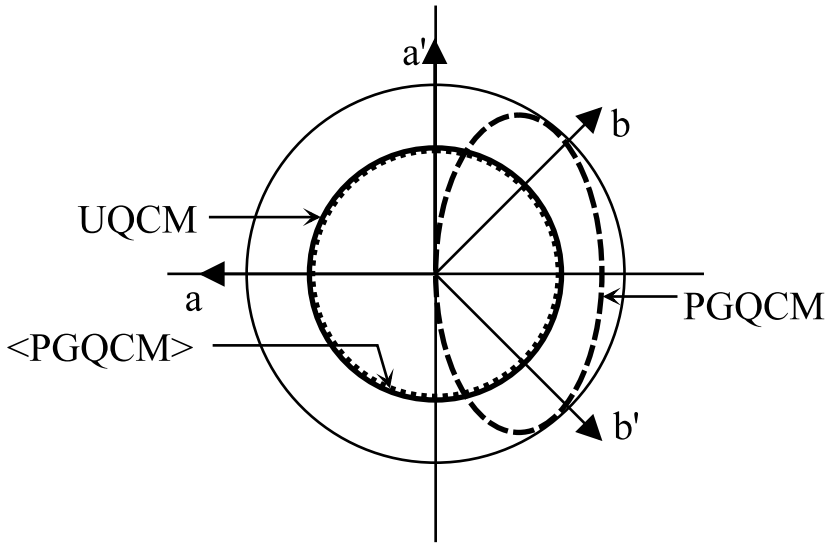

Figure 6:
Bloch vector representation of the states produced by the UQCM (full line), the PGQCM (dashes) and the symmetrized PGQCM (dots) corresponding to input state represented by a large circle on the Poincaré sphere. The directions $\mathbf{a}$, $\mathbf{a}'$, $\mathbf{b}$ and $\mathbf{b}'$ are used for testing the inequality. We see that the choice of the symmetry breaking axis for the PGQCM influences the possible violation of the inequality.